

Airgate Offering Product Authentication Platform

The system is based on tags and interrogators using Hitachi's tiny μ -chip.

By Mary Catherine O'Connor

April 6, 2007—Since [Hitachi](#) first announced its [\$\mu\$ -chip](#) (pronounced "mew-chip") in 2003, the super-small integrated circuit designed for RFID applications has not seen much traction in the United States. The chip operates at 2.45 GHz, can be read from up to roughly 12 inches (30 cm) and holds up to 128 bits of data.

The tag's ID is permanently written and cannot be altered, and the chip does not support an anticollision protocol (which allows the simultaneous reading of multiple tags). Consequently, it is not easily adapted to the types of supply-chain applications for which EPC tags are widely used. However, says Mike Sheriff, president and CEO of [Airgate Technologies](#), the 0.4mm-square chip can be embedded into any object, including paper, and its 128 bits of memory can be used for trillions of unique IDs without duplication, making the μ -chip an attractive tool for authentication applications.

Airgate recently announced the GenuDOT product authentication platform, based on tags carrying the μ -chip. The GenuDOT platform uses inlays and interrogators made for Airgate by Hitachi. Airgate created a Web-based software application to operate on the readers and function as the backbone for the authentication system.

Many end users are using passive HF or UHF tagging systems and encoding unique EPCs to the tags, both for track-and-trace applications and for authentication purposes. Sheriff believes this is the wrong way to go, because the air interfaces are based on open standards (ISO 15693 and ISO 14443 for HF, ISO 18000-6C for UHF). The use of open standards, he says, makes those tags inherently vulnerable to cloning, since someone with an off-the-shelf interrogator could read a number—say, an EPC—off a standard tag used for product authentication, then create another tag using that same number and introduce a fake product into the supply chain. This might even work with encrypted numbers, he adds, if the tag always generates the same encrypted number.

"Our feeling is, encrypted or not, tags that follow published standards are vulnerable to spoofing. You might not be able to read the data, but you can clone it," says Sheriff. "People always say you need open standards, but for a locked-down authentication, you need a proprietary system."

The air-interface protocol used to encode and read Hitachi chips is proprietary, as is the numbering scheme followed by the unique ID encoded to each tag. To deploy the GenuDOT system for an end user, Sheriff says, Airgate will work with Hitachi to designate large batches of IDs for encoding to the tags used to authenticate products. Each of the ID numbers will include special Airgate and Hitachi headers, as well as a unique serial number.

According to Sheriff, as products are manufactured or packaged, an inlay containing the μ -chip will be embedded in each product and encoded with a unique ID. As this happens, the reader will send the unique ID to the Airgate software, where it will be registered as a deployed number linked to a genuine product. The

software will then update the database of deployed numbers to include the new entries. This database is stored on readers deployed further down the supply chain—at distribution centers, retail stores, pharmacies and so forth—and updated through an Internet connection to the main database periodically.

When the products are presented to these readers, the tags are authenticated in three ways. First, if the interrogator cannot read the tag, that signifies it is either broken or does not comply with Hitachi's protocol. (The tag can also be manufactured with a tamper-proof design making it unreadable if it has been removed from an original product and placed on another.) If the interrogator is able to read the tag, it checks to see if it contains an Airgate header, then checks for a unique ID against the most current database of deployed numbers. If it cannot read the tag, or if the tag does not contain a valid ID or header, the reader can either send an audio alert or display a message on its integrated LED screen.

Tags that pass all three tests are approved, and the readers pass a message of authentication along to whatever system the end user has deployed for product tracking. Those that fail any of the tests are diverted out of the supply chain and sent for inspection.

In addition, Airgate has devised a means of authenticating the readers, preventing them from being reverse-engineered by a third party intent on sending false authentication reports to the end user. To accomplish this, the company installs a set of encryption keys each reader must use to establish a connection to the network.

Sheriff says the μ -chip tags have performed reasonably well on products containing metal and liquids. In a demonstration of the tags attached to wine bottles, for instance, the tags could be read from a distance of 1 to 2 inches, despite the liquid contents.

RELATED_ARTICLES The lack of an anticollision protocol means the tags used in a GenuDOT system would not be easily read in large groups, so end users would need to establish business processes designed around reading the tags one at a time. Sheriff does note, however, that Hitachi is developing a new version of the μ -chip with anticollision properties.

According to Sheriff, the price of the tags will depend on a number of variables, including the form factor and size, though he believes companies whose products are being counterfeited would be willing to invest in a system that could protect their brands. A recent [white paper](#) published by [Texas Instruments](#) says counterfeiting and product diversion costs companies \$450 billion a year, globally.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved